TLP:CLEAR
Szabadon terjeszthető!

Kiberfenyegetettség elemzés a NATO tagállamokat érintő geopolitikai eszkalációval összefüggésben

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ-NKI) a balti államokat érintő geopolitikai eszkalációval összefüggésben kiberfenyegetettségi elemzést készített az orosz állami, katonai és államhoz köthető kiberbűnözői tevékenységekről. Az elemzés bemutatja az aktuális geopolitikai helyzetet, a legismertebb támadói csoportok jellemző technikáit, valamint az NBSZ-NKI által javasolt védekezési intézkedéseket.

A Kreml 2026 májusának végén válaszlépések alkalmazását helyezte kilátásba, miután azzal vádolta Ukrajnát, hogy Lettország légterét és területét dróntámadások előkészítésére vagy indítására használja. Egy nappal korábban orosz hírszerzési források azt állították, hogy Lettország NATO-tagsága nem nyújt védelmet egy esetleges orosz megtorlással szemben. Az ilyen típusú politikai-katonai eszkaláció növeli annak kockázatát, hogy orosz állami vagy államhoz köthető szereplők kibereszközökkel is nyomást gyakoroljanak a balti államokra, illetve a NATO- és EU-tagállamok közös katonai és gazdasági övezetéhez kapcsolódó szervezetekre.

A támadók célja nem feltétlenül az azonnali, jelentős mértékű károk előidézése, hanem hozzáférések kiépítése, szolgáltatások zavarása, a reagálási képességek felmérése, hírszerzési előny szerzése, valamint a közbizalom gyengítése lehet.

Kiberfenyegetési szempontból kiemelt kockázatot jelentenek az orosz állami vagy államhoz köthető szereplők – különösen a Turla, az APT28 és az APT29 – , mivel korábbi európai tevékenységük alapján képesek célzott hozzáférésszerzésre, hírszerzésre és hosszabb távon aktiválható műveleti jelenlét kialakítására. A kockázat elsősorban azoknál a szervezeteknél jelentkezik, amelyek internet felől elérhető tűzfalakat, VPN-eket, e-mail szolgáltatásokat, webmail-felületeket, webportálokat, identitáskezelő rendszereket, peremeszközöket (edge device) vagy távoli adminisztrációs megoldásokat üzemeltetnek.

Ügyfeleinknek ezért javasolt kiemelt figyelmet fordítaniuk az internet felől elérhető rendszerek, a privilegizált hozzáférések, a beszállítói kapcsolatok felülvizsgálatára, valamint az elosztott szolgáltatás-megtagadásos támadások (DDoS) elleni ellenálló képesség kialakítására.

Támadási minta elemzés

A MITRE ATT&CK elemzés alapján az orosz állami hátterű vagy ahhoz kapcsolódó szereplők – kiváltképp a Turla, az APT28 és az APT29 – műveleteiben visszatérő mintázatként jelenik meg az internet felől elérhető rendszerek kompromittálása (T1190), a célzott adathalászat (T1566), a hitelesítő adatok megszerzésére irányuló jelszó-próbálgatásos támadások (T1110), valamint a kompromittált rendszereken végzett credential dumping (T1003), valamint legitim fiókokkal történő hozzáférésszerzés (T1078), külső távoli szolgáltatásokon keresztüli bejutás és perzisztencia (T1133), valamint fiókok manipulálásával történő tartós jelenlét kiépítése (T1098). A támadók gyakran alkalmaznak hamis bejelentkezési felületeket, ellopott vagy

újrahasznosított hitelesítő adatokat, illetve privilegizált beszállítói hozzáférésekkel való visszaélést.

A csoportok jellemzően PowerShell, script és parancsértelmező-alapú végrehajtást alkalmaznak (T1059), majd rejtett, proxyzott vagy tunneling alapú kommunikációs csatornákon keresztül tartják fenn a kapcsolatot a kompromittált infrastruktúrával (T1071, T1090, T1105). Gyakori elem továbbá a rendszerszintű felderítés: fájlok és könyvtárak (T1083), futó folyamatok (T1057), valamint jogosultsági csoportok feltérképezése (T1069), az oldalirányú mozgás távoli szolgáltatásokon keresztül (T1021), valamint az adatok archiválása és fokozatos kiszivárogtatása (T1560, T1048, T1567). A műveletek során kiemelt szerepet kapnak a védelemkijátszási technikák, például folyamatmaszkolás, nyomeltüntetés és legitim adminisztrációs eszközök használata (T1036, T1070, T1218).

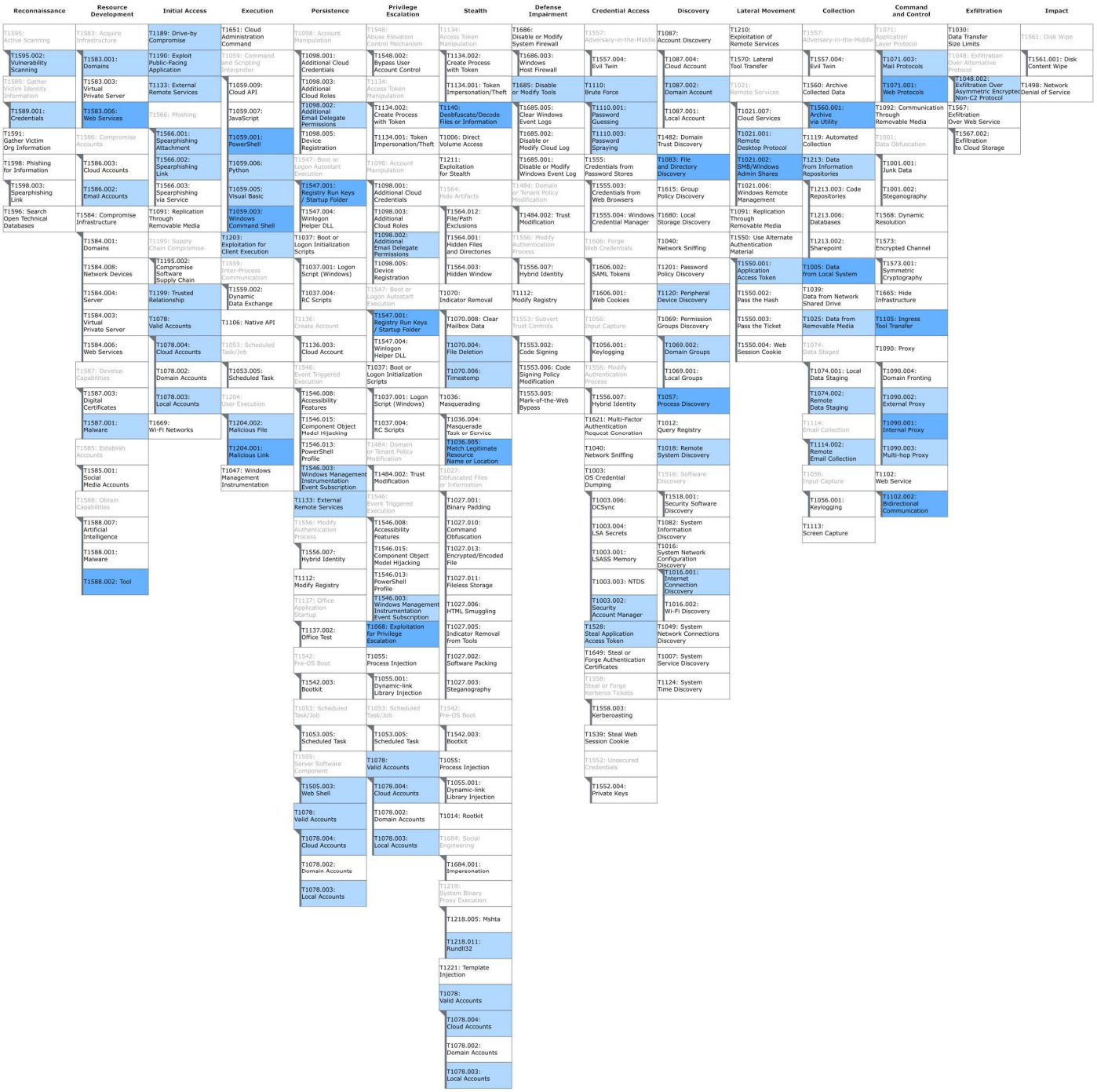
Az elemzett minták alapján a támadók elsődleges célja nem feltétlenül az azonnali károkozás, hanem a hosszú távú, rejtett hozzáférés fenntartása, az információszerzés, valamint szükség esetén zsarolási, reputációs vagy befolyásolási célú műveletek támogatása. Ezzel párhuzamosan továbbra is számolni kell DDoS-jellegű túlterheléses támadásokkal, hack-and-leak műveletekkel, illetve ransomware vagy adatlopással kombinált zsarolási kísérletekkel is, különösen olyan szervezetek esetében, amelyek nyilvános szolgáltatásokat, kritikus infrastruktúrát vagy nagy mennyiségű érzékeny adatot kezelnek.

A fenti MITRE ATT&CK minták és a jelenlegi geopolitikai környezet alapján megnövekedett kockázattal kell számolni különösen az alábbi kibertevékenységek esetében:

- hitelesítőadat-lopás és célzott adathalászat;
- hamisított belépési oldalak használata, különösen webmail, VPN és felhős szolgáltatások esetén;
- internet felől elérhető tűzfalak, VPN-ek, e-mail rendszerek, webportálok és peremeszközök (edge device) kompromittálása;
- perzisztens hozzáférések kiépítése;
- tunneling és rejtett távoli hozzáférési csatornák használata;
- privilegizált vagy beszállítói fiókokkal való visszaélés;
- DDoS- és hacktivista jellegű túlterheléses támadások;
- ransomware vagy adatlopással kombinált zsarolási kísérletek;
- hack-and-leak műveletek, kiszivárogtatás, reputációs támadás;
- kiberműveletek összehangolása befolyásolási vagy fizikai incidensekkel.

TLP:CLEAR

Szabadon terjeszthető!



1. ábra: A három csoport (Turla, APT28, APT29) támadási technikái aggregált formában láthatók: a sötétebb szín magasabb előfordulási gyakoriságot vagy több csoport általi alkalmazást jelez. Forrás: MITRE ATT&CK® Navigator

Ajánlott intézkedések

Az NBSZ-NKI a fenyegetettséggel összefüggésben az alábbi intézkedések megtételét javasolja. Általánosságban elmondható, hogy az itt felsoroltak alkalmazása érdemben tudja javítani a szervezetek kibertámadások elleni rezisztenciáját.

MFA kötelező alkalmazása
A szervezetek haladéktalanul vezessenek be, vagy tegyenek kötelezővé többfaktoros hitelesítést minden kritikus hozzáférésnél.

Kiemelten érintett hozzáférések:

- adminisztrátori fiókok;
- VPN- és távoli hozzáférések;
- e-mail és webmail rendszerek;
- felhős adminfelületek;
- identitáskezelő rendszerek;
- privilegizált hozzáférések;
- beszállítói és karbantartói hozzáférések.

A hagyományos SMS- vagy push-alapú MFA önmagában nem tekinthető elegendőnek magas kockázatú hozzáférések esetén. Ahol lehetséges, FIDO2/WebAuthn, hardverkulcsos vagy más phishing-rezisztens megoldás alkalmazása javasolt.

Internet felől elérhető rendszerek azonnali felülvizsgálata és kitettségcsökkentése
A szervezetek készítsenek leltárt minden internet felől elérhető szolgáltatásról, és csökkentsék a szükségtelen kitettséget.

Kiemelten vizsgálandó rendszerek:

- tűzfalak;
- VPN-ek;
- e-mail gatewayek;
- webmail / OWA felületek;
- publikus webportálok;
- távoli adminisztrációs felületek;
- identitás- és hozzáféréskezelő portálok;
- peremeszközök (edge device);
- felhős menedzsmentkonzolok;
- fájlmegosztó és collaboration rendszerek.

Ajánlott intézkedések:

- nem használt szolgáltatások letiltása;
- adminisztrátori felületek internetes elérésének megszüntetése;
- hozzáférés korlátozása IP-cím vagy megbízható hálózat alapján;
- adminisztrátori portálok VPN, zero-trust vagy más védett hozzáférési réteg mögé helyezése;

- elavult vagy nem támogatott rendszerek kiváltása;
- külső támadási felület rendszeres ellenőrzése.

Fenyegetésvezérelt sérülékenységkezelés
A szervezetek javítsák a gyakran kihasznált, különösen internet felől elérhető rendszereket érintő sérülékenységeket.

Priorizálni szükséges az alábbi rendszereket:

- VPN és távoli hozzáférési megoldások;
- tűzfalak és edge security appliance-ek;
- e-mail és webmail rendszerek;
- webes portálok;
- identitáskezelő rendszerek;
- virtualizációs és felhős menedzsmentplatformok;
- fájlmegosztó és együttműködési szolgáltatások.

A havi vagy rutinszerű patch-ciklus önmagában nem elegendő. A magas kockázatú, aktívan kihasznált vagy széles körben célzott sérülékenységeket gyorsított eljárásban kell kezelni. Az NBSZ-NKI rendszeresen tesz közzé weboldalán sebezhetőségi információkat, melyeket javasolt napi szinten követni.

Feltételes és kockázatalapú hozzáférés bevezetése
A hozzáféréseket kockázatalapú szabályokkal szükséges védeni. Nem elegendő a felhasználónév, jelszó és MFA kombinációjára hagyatkozni.

Ajánlott kontrollok:

- magas kockázatú országokból érkező belépések blokkolása vagy külön ellenőrzése;
- TOR, anonimizáló VPN, proxy és adatközponti IP-k szigorú kezelése;
- új eszközről vagy szokatlan helyről történő belépés újrahitelesítése;
- adminisztrátori felületek elérése csak jóváhagyott eszközről és hálózatból;
- privilegizált műveletekhez dinamikusan megjelenő kiegészítő hitelesítés (step-up authentication);
- feltételes hozzáférési szabályok rendszeres felülvizsgálata.

Privilegizált hozzáférések szegmentálása és szigorítása
A kiemelt jogosultságokat javasolt minimálisra csökkenteni, külön kezelni és folyamatosan monitorozni.

Ajánlott intézkedések:

- napi használatú fiókok és adminisztrátori fiókok szétválasztása;
- domain admin és global admin jogok minimalizálása;
- Just-in-Time és Just-Enough-Administration alkalmazása;
- külön adminisztrátori fiókok használata kritikus rendszerekhez;
- privilegizált munkamenetek naplózása;
- adminisztrátori tevékenység riasztásalapú monitorozása;
- inaktív vagy indokolatlan adminisztrátori jogok visszavonása;
- beszállítói adminisztrátori jogok időbeli és funkcionális korlátozása.

Perzisztens hozzáférések, tunneling és anomáliák keresése
A szervezetek auditálják rendszereiket olyan hozzáférések azonosítását keresve, amelyeket későbbi hírszerzési vagy zavaró műveletekhez használhatnak fel.

Keresendő minták:

- ismeretlen vagy ritkán használt távoli kapcsolatok;
- szokatlan tunneling forgalom;
- nem dokumentált VPN- vagy proxykapcsolatok;
- hosszú életű, alacsony zajszintű hálózati kapcsolatok;
- szokatlan outbound forgalom kritikus rendszerekről;
- peremeszközök (edge device) konfigurációmódosítások;
- újonnan létrehozott adminfiókok;
- nem jóváhagyott remote management eszközök;
- naplózás leállítása, törlése vagy csökkentése;
- szokatlan szolgáltatásfiók-használat.

Távoli menedzsment aktivitás fokozott monitorozása
A távoli adminisztrációs tevékenységeket külön kockázati kategóriaként indokolt kezelni, ezen belül az alábbiakra szükséges figyelmet fordítani:

- szokatlan RDP, SSH, VPN vagy adminisztrátori portál-belépésekre;
- munkaidőn kívüli adminisztrátori tevékenységre;
- tömeges konfigurációmódosításokra;
- új távoli menedzsment eszközök telepítésére;
- szokatlan fájlmozgásokra;
- beszállítói fiókok rendellenes aktivitására;
- peremeszközök (edge device) beállításainak módosítására;
- távoli hozzáférési szolgáltatások degradációjára vagy manipulációjára.

DDoS-védelem megerősítése
A DDoS-támadások célja nem kizárólag a technikai rendelkezésre állás ellehetetlenítése lehet, hanem az intézmény megbízhatóságba vetett bizalom gyengítése is. Ezért a DDoS-védelmet üzletmenet-folytonossági és válságkommunikációs kérdésként is kezelni kell.

Ajánlott intézkedések:

- DDoS-mitigációs szolgáltató előzetes bevonása;
- CDN és forgalomszűrés alkalmazása;
- autoscaling biztosítása kritikus webes szolgáltatásoknál;
- upstream szolgáltatókkal előre egyeztetett eszkaláció;
- alternatív kommunikációs csatornák kijelölése;
- szolgáltatáskimaradásra vonatkozó kommunikációs sablonok előkészítése;
- DDoS-gyakorlatok vagy technikai tesztek végrehajtása.

Beszállítói és harmadik feles hozzáférések felülvizsgálata
A kritikus beszállítók és szolgáltatók hozzáférései kiemelt kockázatot jelentenek. A szervezetek vizsgálják felül minden harmadik fél hozzáférését, különösen karbantartók, IT-outsourcing partnerek, védelmi beszállítók, logisztikai partnerek és közlekedési rendszereket támogató szolgáltatók esetén.

Elvárható minimumkövetelmények:

- MFA;
- naplózási követelmények teljesítése;
- privilegizált hozzáférések szegmentálása;
- távoli menedzsmenttevékenység monitorozása;
- incidensjelentési kötelezettség;
- hozzáférések rendszeres felülvizsgálata;
- ideiglenes hozzáférések automatikus lejárata;
- hozzáférések azonnali visszavonása szerződés vagy feladat lezárásakor.

Naplózás, észlelés és riasztási szabályok megerősítése
A szervezetek vizsgálják meg és biztosítsák, hogy a kritikus rendszerek naplózása teljes, központilag gyűjtött és visszamenőlegesen vizsgálható legyen.

Kiemelten naplózandó események:

- sikeres és sikertelen bejelentkezések;
- privilegizált műveletek;
- adminisztrátori jogok kiosztása és visszavonása;
- MFA-módosítások;
- új fiókok létrehozása;
- szolgáltatásfiókok használata;
- VPN- és távoli hozzáférési események;
- konfigurációmódosítások;
- naplózás kikapcsolása vagy módosítása;
- adatletöltési és tömeges fájlmozgási események.

A naplókat védeni szükséges törlés, módosítás és jogosulatlan hozzáférés ellen.

Incidens és befolyásolási művelet együttes kezelése
Egy incidens reputációs vagy akár információs művelettel is párosulhat, ezért incidens esetén nem elegendő kizárólag technikai vizsgálatot indítani.

Párhuzamosan vizsgálandó:

- adatlopás vagy kiszivárogtatás lehetősége;
- hack-and-leak narratívák megjelenése;
- hamisított dokumentumok terjedése;
- közösségi médiás dezinformáció;
- célzott reputációs támadás;
- vezetők, alkalmazottak vagy beszállítók doxolása;

- DDoS- és propagandaaktivitás egyidejű megjelenése.

A kiberbiztonsági, kommunikációs, jogi, adatvédelmi, valamint vezetői válságkezelési folyamatokat ajánlott egységesen kezelni.

NBSZ-NKI CSIRT koordináció előkészítése
A szervezetek számára javasolt előzetesen meghatározni, hogy incidens esetén kivel, milyen kommunikációs csatornán, valamint milyen döntéshozatali rend szerint történik a kapcsolatfelvétel.

Előkészítendő:

- NBSZ-NKI CSIRT-kapcsolat;
- internetszolgáltatói eszkaláció;
- felhőszolgáltatói eszkaláció;
- DDoS-mitigációs szolgáltató kapcsolata;
- jogi és adatvédelmi kapcsolattartók;
- kommunikációs és sajtókapcsolati felelősök;
- vezetői döntéshozói ügyeleti rend.

Az eszkalációs listákat naprakészen kell tartani és rendszeresen tesztelni kell.

Üzletmenet-folytonossági és helyreállítási képességek tesztelése
A szervezetek ne csak dokumentálják, hanem gyakorolják is a kritikus szolgáltatások kiesésére vonatkozó eljárásokat.

Gyakorlandó incidenskezelési forgatókönyvek:

- e-mail nélküli működés;
- VPN-kiesés;
- DDoS alatti ügyfél- és lakossági kommunikáció;
- ransomware utáni helyreállítás;
- kritikus rendszerek izolálása;
- kézi vagy alternatív üzemeltetési mód;
- mentésekből történő visszaállítás;
- hatósági bejelentési folyamat;
- nyilvános kommunikáció reputációs támadás esetén.

A mentéseket rendszeresen tesztelni szükséges, a mentési környezetet pedig el kell különíteni az éles rendszerektől, és védeni kell a jogosulatlan módosítással vagy törléssel szemben.

Fenyegetettségi információk követése és szervezetspecifikus támogatás
A szervezetek számára javasolt a releváns fenyegetettségi információk folyamatos nyomon követése, különös tekintettel a kritikus infrastruktúrákat, valamint a kormányzati, közlekedési, logisztikai, energetikai, pénzügyi és telekommunikációs szektorokat érintő biztonsági eseményekre és incidensekre.

Az NBSZ NKI javasolja, hogy az érintett szervezetek rendszeresen kövessék az NBSZ-NKI weboldalán közzétett riasztásokat, tájékoztatókat és fenyegetettségi információkat, valamint használják fel a havi CTI elemzésekben szereplő megállapításokat saját védelmi intézkedéseik, detektálási szabályaik és kockázatértékelésük aktualizálásához.

A jogosult, kritikus infrastruktúrát üzemeltető szervezetek soron kívüli, szervezetspecifikus fenyegetettségelemzést kérhetnek az NBSZ-NKI-tól a cyberthreat@nki.gov.hu e-mail címen.

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833